FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
211526US2PCT	09/889557

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR00/00174	26 January 2000	27 January 1999

TITLE OF INVENTION

AUTHENTICATION OR SIGNATURE PROCESS WITH A REDUCED CALCULATIONS SET

APPLICANT(S) FOR DO/EO/US

Marc GIRAULT, et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☒ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

PCT/IB/304 **Amended Sheets (Pages 5, 6, 7, 13, 14 and 15)**
PCT/IB/308
Notice of Priority
Request for Consideration of Documents Cited in the International Search Report

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/889557	PCT/FR00/00174	211526US2PCT

24. The following fees are submitted:.		CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :			
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1000.00**		
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	**$860.00**		
☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**		
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**		
☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =		**$860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	7 - 20 =	0	x $18.00	**$0.00**	
Independent claims	2 - 3 =	0	x $80.00	**$0.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$860.00**	
☐ Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$860.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				**$0.00**	
TOTAL NATIONAL FEE =				**$860.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				**$0.00**	
TOTAL FEES ENCLOSED =				**$860.00**	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of **$860.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **15-0030** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Telephone: (703)413-3000
Fax: (703)413-2220

22850

Surinder Sachar
Registration No. 34,428

Surinder Sachar
SIGNATURE

Marvin J. Spivak
NAME

24,913
REGISTRATION NUMBER

7-27-01
DATE

211526US

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF :

MARC GIRAULT ET AL : ATTN: APPLICATION DIVISION

SERIAL NO: NEW U.S. PCT APPLICATION :

(Based on PCT/FR00/00174)

FILED: HEREWITH :

FOR: AUTHENTICATION OF SIGNATURE PROCESS WITH A REDUCED CALCULATIONS SET :

PRELIMINARY AMENDMENT

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Prior to a first examination on the merits, please amend the above-identified application as follows:

IN THE CLAIMS

Please cancel Claims 1-7 without prejudice.

Please add new Claim 8-14 as follows:

8. (New) An authentication process involving a first entity, which possesses a public key v and a secret key s, the public and secret keys being related by an operation modulo n, where n is an integer, the modulus n being specific to the first entity, and a second entity, which knows the public key v, the first and second entities being provided with means to exchange zero-knowledge information and to carry out cryptographic calculations on the

zero-knowledge information, calculations being carried out modulo n, wherein in the process the modulo n operation is of $v=s^{-t} \pmod n$, t being a parameter.

9. (New) A process according to claim 8, wherein the information exchanges are of zero-knowledge and wherein the cryptographic calculations are completed as follows:

the first entity selects at least one integer r at random ranging between 1 and n-1 and calculates at least one parameter x equal to $r^t \pmod n$, then at least one number c that is at least one function of the at least one of a parameter and a message, and sends the at least one number c to the second entity;

the second entity receives the at least number c, selects at least one number e at random, and sends the at least one number e to the first entity;

the first entity receives the at least one number e, carries out at least one calculation using the at least one number e and the secret key s, the result of the at least one calculation yielding at least one answer y, and sends the at least one answer y to the second entity.

the second entity receives the at least one answer y, carries out one calculation using the public key v and the modulus n, and checks with a modulo n operation that the result of the one calculation is coherent with the received at least one number c.

10. (New) A process according to Claim 9, wherein a size of the number n, expressed in number of bits, is less than 1,000.

11. (New) A process according to Claim 10, wherein a size of the number n is between 700 and 800.

12. (New) A process according to Claim 8, wherein n is a product of at least two primes, and wherein the modulo n calculations are performed according to a Chinese remainders method.

13. (New) A message signature process configured for a signatory provided with a public key v and a secret key s, the public and private keys being related by a modulo n calculation, where n is an integer, which is specific to the signatory, the process utilizing means configured to calculate at least one number c that is a function of a message M to be signed, configured to calculate at least one number y that is a function of the secret key s, and configured to transmit the numbers y and c that are the signature of the message and the message M, wherein the modulo n operation is $v=s^{-t} \pmod n$, t being a parameter.

14. (New) A message signature process according to claim 13, wherein the signatory selects an integer r at random between 1 and n-1, calculates a parameter x equal to $r^t \pmod n$, calculates at least one number e that is a function of parameter x and the message M to be signed, calculates the at least one number y using its secret key s, said at least one number y being a function of numbers r and e, and transmits the numbers c and y as the signature.

REMARKS

Favorable consideration of this application, as presently amended, is respectfully requested.

The present preliminary amendment cancels Claims 1-7 and sets forth new Claims 8-14 for examination. New Claims 8-14 are deemed to be self-evident from the original disclosure, and thus are not deemed to raise any issues of new matter.

The present application is believed to be in condition for a full and thorough examination on the merits. An early and favorable consideration of the present application is hereby respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

(703) 413-3000
Fax No.: (703)413-2220
GJM/SNS:kst

I:\atty\SNS\211526us-pr.wpd

Marked-Up Copy
Serial No:

Amendment Filed on:
07-27-01

IN THE CLAIMS

--Claims 1-7 (Cancelled).

Claims 8-14 (New).--

Authentication or signature process with a reduced calculations set.

Technical domain

The present invention relates to an authentication or signature process with a reduced calculations set.

More precisely, the invention relates to the public key cryptography domain. Following this process, the entity to be authenticated - the prover - possesses a secret key and an associated public key. The authenticating entity - the verifier - only needs this public key to achieve the authentication.

Even more precisely, the process relates to the set of processes called "Zero-knowledge Protocols", i.e. without any communication of knowledge. According to this kind of process, the authentication is carried out following a protocol that, as it is recognised, and under assumptions considered as perfectly reasonable by the scientific community, discloses nothing about the secret key of the prover.

To be even more precise, the invention relates to zero-knowledge processes based on factoring problems (i.e. on the difficulty to factor large integers into a product of prime numbers).

The invention is applicable in every system where it is necessary to authenticate parties or messages, or to sign messages, in particular in systems where the amount of calculations to be carried out by the prover is critical. This is especially the case for cards that use a standard microprocessor or low cost cards, with no arithmetic coprocessor (which are often called

cryptoprocessor) where cryptographic calculations must be accelerated.

A typical application of the invention is the electronic purse that requires a very high security level while discarding the use of a cryptoprocessor, either because of the cost or for technical reasons (for example the use of a contact-less interface), or both.

Another possible application is the next generation telecard, whose cost constraints are by far stricter than those of the electronic purse.

Prior art

A number of zero-knowledge identification processes have been published. For example:

- The FIAT-SHAMIR protocol described in the article by A. FIAT and A. SHAMIR entitled "how to prove yourself: Practical solutions to identification and signature problems", published in "Advances in Cryptology: Proceedings of CRYPTO'86, Lecture Notes in Computer Science", vol. 263, Springer-Verlag, Berlin, 1987, pp. 186-194,
- The GUILLOU-QUISQUATER protocol, described in the article by L.C. GUILLOU and J.J. QUISQUATER, entitled "A Practical zero-knowledge protocol fitted to security microprocessors minimising both transmission and memory, published in "Advances in Cryptology: Proceedings of EUROCRYPT'88; Lecture notes in Computer Sciences, vol. 330, Springer-Verlag, Berlin, 1988, pp. 123-128,

- The GIRAULT protocol described in the French patent application FR-A-2 176 058, based on the discrete logarithm problem.

Generally speaking, most zero-knowledge identification (or message authentication) protocols involve three steps. For the sake of simplicity, we shall assume that the verifier B already knows all the public parameters related to the prover A, i.e. its identity, its public key and so on.

As a first transaction, A supplies B with a value "c" called "opening", image through a pseudo-random function h of a parameter x (itself derived from a number r selected by A at random), as well as with the message to be authenticated or signed: $c = h(x,[M])$, where the symbol [M] means that M is optional. This is the first step. Some protocols may involve several openings.

During a second transaction, B sends to A a parameter e selected at random (the "question"). It is the second step.

During a third transaction, A sends to B an "answer" y that is in coherence with the question e, the opening c and the secret key of A (third step).

Then B checks the received answer. More precisely, B recalculates x from the elements y, e and v using the relation $x=\varphi(y,e,v)$ and verifies that $c=h(\varphi(v,e,y),[M])$, which is the fourth step.

When there is no message to authenticate, the use of the pseudo-random function h is optional. In this case, c=x is convenient. The verification consists of checking that $x=\varphi(y,e,v)$.

In some protocols, there are one or two more transaction(s) between the verifier and the prover.

For a message signature, the two first steps are discarded, as the parameter e is made equal to c; A then successively and only calculates c, e(=c) and y.

The number u of questions to be answered depends directly on the desired protocol security level. This level is defined as the probability p of detecting an impostor. (i.e. an entity C that fraudulently mimics A). It is measured by a parameter k whose value is related to p by the relation $p=1-2^{-k}$. In other words, the impostor only has 1 chance in 2^k of succeeding. It can be demonstrated in the present case that if a protocol relies on a difficult mathematical calculation, and if the openings are of adequate length, the length of u must simply equal k bits. A typical value of k is 32, which gives the impostor one chance in 4 billion to be successful. In applications where the failure of an identification may have very harmful consequences (e.g. legal proceedings), this length may be reduced to a few bits.

For protocols using factoring, the calculation of x in terms of r, or the calculation of y in terms of e, or both, involve(s) operations modulo n, where n is a compound number that is hard to factor. This number is said to be of the universal type, generated by a trustworthy third party. It is stored and used by all authorised entities. The "universal" character of n implies that it is a large number (usually 1024 bits), as breaking the factoring of n should compromise the secret keys of all accredited users.

English translation of the amended sheets of International Preliminary Examination Report

In their basic versions, none of the above mentioned protocols can be implemented in an application that has to comply with severe specifications (low cost, low sophistication), as described in the previous section, as the required calculations could not be performed by a microprocessor card without a cryptoprocessor.

Though the French patent application FR-A-2 752 122 describes an optimisation of these protocols, it is restricted to protocols involving the discrete logarithm method following a mode called "with pre-calculations" that has the drawback of implying regularly scheduled reloads.

The document from J. BRANDT et al. entitled "zero-knowledge Authentication scheme with Secret Key Exchange" published in Advances in Cryptology, Crypto 88 Proceedings, XP 000090662, pp. 583-588, describes a zero-knowledge authentication scheme with exchange of secret keys between two users, a scheme wherein the prover calculates its own modulus $n=pq$ and carries out an operation of the type $m^d \pmod n$.

The present invention aims to reduce the number of calculations to be carried out by the prover when using zero-knowledge identification (or message signature or authentication) protocols involving factoring, the gain being liable to reach a factor 2 or 3 when using a particular operation $v=s^{-t} \pmod n$.

It also makes possible - and in particular when coupled with the GUILLOU-QUISQUATER protocol - the fast completion of an identification (or message authentication or signature) with public key included in a low cost standard microcircuit card, for applications such as the electronic purse or next generation telecard.

English translation of the amended sheets of International Preliminary Examination Report

Description of the invention

The modulus n being an individual parameter (in other words each user owns his own n value), this selection may be exploited in the following two ways (which may be advantageously combined):

1) first by retaining a length of n lower than the currently used values (typically lower than 1000 bits and for example, ranging between 700 and 800 bits); this is possible as breaking the factoring of n only compromises the secret key of the related user and in no way the secret keys of other users; this modification alone reduces the duration of calculations carried out modulo n by 40%;

2) If the user has stored the prime factors of n in the memory of his security device, he may use the Chinese remainders technique to further reduce the duration of modulo n calculations by 40%, when there are two prime factors; this reduction may be increased when using several prime factors (typically 3 or 4).

On the whole, the modulo n calculations can then be reduced by 60%, that is a factor 2, at least.

Precisely, the invention relates to a process of identification involving a first entity called a "prover", owning a public key v and a secret key s, these keys being related by a modulo n calculation, where n is an integer called modulus, specific to the prover, and a second entity called a "verifier", which knows the

English translation of the amended sheets of International Preliminary Examination Report

public key v, these entities being provided with means to exchange information in a zero-knowledge context and to carry out cryptographic calculations on this information, some calculations being performed in the modulo n mode, the process being characterised by the fact that the modulus of the modulo n operation expressed as $v=s^{-t} \pmod n$, t being a parameter.

The aforementioned entities may be, for example, microcircuit cards, electronic purses, telecards, and so on...

Following a preferred implementation, the zero-knowledge information exchanges and the cryptographic calculations are as follows:

- the prover selects one (several) integer(s) r at random ranging between 1 and n-1 and calculates one (several) parameter(s) x equal to $r^t \pmod n$, then one (several) number(s) c called opening(s) that is (are) one (several) function(s) of this (these) parameter(s) and possibly of a message (M), and sends this (these) opening(s) to the verifier;
- the verifier entity receives the opening(s) c, selects one number e at random called "question" and sends this question to the prover;
- the prover receives the question e, carries out one (several) calculation(s) using this question e and the secret key s, the result of this (these) calculation(s) yielding one

(several) answer(s) $\underline{y}$, and sends this (these) answer(s) to the verifier.

- The verifier receives the answer(s) $\underline{y}$, carries out one calculation using the public key $\underline{v}$ and the modulus $\underline{n}$, and checks with a modulo $\underline{n}$ calculation that the result is coherent with the received opening(s).

The size of the number n, expressed in number of bits, is less than 1000. For example, it may be between 700 and 800.

The present invention also relates to a message signature process to be used by an entity called a "signatory", this entity being provided with a public key $\underline{v}$ and a secret key $\underline{s}$, which are related by a modulo $\underline{n}$ operation, where $\underline{n}$ is an integer called modulus and $\underline{t}$ is a parameter, a process in which the signatory calculates an opening $\underline{c}$ that is notably a function of the message to be signed and a number $\underline{y}$ that is a function of the secret key, transmits the numbers $\underline{y}$ and $\underline{c}$ that are the signature and the message, the process being characterised in that the modulus n is specific to the signatory.

Following a preferred implementation, the signatory selects an integer $\underline{r}$ at random between 1 and n-1, calculates a parameter $\underline{x}$ equal to $r^t \pmod{n}$, calculates a number $\underline{c}$ that is a function of the parameter $\underline{x}$ and of the message to be signed, calculates a number $\underline{y}$ using the secret key $\underline{s}$, as a function of numbers $\underline{r}$ and $\underline{e}$, then transmits the numbers $\underline{c}$ and $\underline{y}$ as signature.

Detailed description of particular implementations for the invention

In the following description, the invention is assumed to be combined with the protocol GUILLOU-QUISQUATER, as an example. It is clear that the invention is not restricted to this protocol.

Note that the universal parameters of the GUILLOU-QUISQUATER protocol are the modulus n, products of prime numbers, comprising at least 1024 bits, and an integer value t.

The public key v and the secret key s verify the relation $v=s^{-t} \pmod n$.

The retained security level is u (lower than or equal to t, commonly equal to t)

The authentication of A by B, which are named Alice and Bob, following the usual terminology, is completed as follows:

1. Alice selects r within the range [1,n-1], calculates $x=r^t \pmod n$ then c=h(x,[M]) and sends c to Bob.
2. Bob selects e within the range [1,u-1] and sends e to Alice.
3. Alice calculates $y=rs^e \pmod n$ and sends y to Bob.
4. Bob calculates $x=y^t v^e \pmod n$ and verifies that c=h(x,[M])

When no message is to be authenticated, it is optional to involve the pseudo random function h: c=x can be used. The verification then consists of checking that $x=y^t v^e \pmod n$.

In the protocol modified in accordance with the invention, t is the only universal parameter.

The public key is (n,v), where n has at least 768 bits. The public key v and the secret key of Alice satisfy the relation $v=s^{-t} \pmod n$.

The secret key may include prime factors from n to take advantage of the second aspect of the invention.

The parameter t may be included in the public key (in this case, there is no longer any universal parameter).

The security level retained by Alice and Bob is u (lower than or equal to t; usually u=t).

The authentication of Alice by Bob is performed as described above, but with faster calculations, which results from a smaller modulus n.

As all Alice's calculations are carried out modulo n, the gain factor resulting from only one modular multiplication affects the complete set of calculations completed by Alice when carrying out the protocol. This should be the same, for example, with Fiat-Shamir or Girault protocols (in the latter case, no gain should be expected in step 3, as there is no modular computation, but the execution time of this step is negligible with respect to the modular exponentiation of the first one).

The invention may also be implemented by the Chinese remainders technique, which consists of calculating the values modulo n of the prime factors of n. As these numbers are inevitably smaller, these operations are quickly done. The result modulo n is still to be obtained through a "reconstitution" operation. This technique is described in the article

of J.J QUISQUATER and C.COUVREUR entitled (Fast Decipherment algorithm for RSA public-key cryptosystem" published in "Electronic Letters", vol. 18, October 1982, pp. 905-907.

Let's consider the case when n is the product of two prime factors p and q.

From the Bezout theorem, it is known that two integers exist, such as ab+bq=1.

To calculate $y=x^e \pmod n$, we start by reducing x modulo each prime factor by calculating $x_p=x \pmod p$ and $x_q=x \pmod q$. We also reduce e modulo (p-1) and (q-1) by calculating $e_p=e \bmod (p-1)$ and $e_q=e \bmod (q-1)$ (in the protocol of Guillou-Quisquater, e is always lower than p-1 and q-1, then $e_p=e_q=1$).

We then calculate $y_p=x_p^{e_p} \pmod p$ and $y_q=x_q^{e_q} \pmod q$. When p and q are of similar size, each of these calculations is about 8 times faster than the calculation $y=x^e \pmod n$ when e and n are of similar size (first case); 4 times faster when the size of e is lower than or equal to the size of p (second case as, for example, in the algorithm). The set of two calculations is then either 4 times faster or 2 times faster.

y is still to be reconstructed from y_p and y_q, which is carried out using the relation:

$$y=y_p+ap(y_q-y_p) \pmod n$$

On the whole, the method of Chinese remainders leads to an acceleration of calculations by a factor

ranging from 3 to 4 in the first case, and from 1.5 to 2 in the second case, when the number of prime factors (assumed to be of similar sizes) is larger than 2 and equal to k; the acceleration factor is nearing k^2 in the first case and close to k in the second case.

English translation of the amended sheets of International Preliminary Examination Report

Claims

1. Authentication process involving a first entity said "prover" (A), which possesses a public key v and a secret key s, these keys being related by an operation modulo n, where n is an integer called modulus, the modulus n being specific to the prover (A), and a second entity called a "verifier" (B), which knows the public key v, these entities being provided with means to exchange zero-knowledge information and carry out cryptographic calculations on this information, some calculations being carried out modulo n, the process being characterised in that the modulo n operation is of the kind $v=s^{-t} \pmod n$, t being a parameter.

2. Process according to claim 1, wherein the information exchanges are of zero-knowledge type and wherein the cryptographic calculations are completed as follows:

- the prover (A) selects one (several) integer(s) r at random ranging between 1 and n-1 and calculates one (several) parameter(s) (x) equal to $r^t \pmod n$, then one (several) number(s) c called opening(s) that is (are) one (several) function(s) of this (these) parameter(s) and possibly of a message (M), and sends this (these) opening(s) to the verifier (B);
- the verifier entity (B) receives the opening(s) c, selects one number e at

random called "question" and sends this question to the prover (A);

- the prover (A) receives the question e, carries out one (several) calculation(s) using this question e and the secret key s, the result of this (these) calculation(s) yielding one (several) answer(s) y and sends this (these) answer(s) to the verifier (B).
- The verifier (B) receives the answer(s) y, carries out one calculation using the public key v and the modulus n, and checks with a modulo n calculation that the result is coherent with the received opening(s).

3. Process according to claim 2, wherein the size of the number n, expressed in number of bits, is less than 1 000.

4. Process according to claim 3, wherein the size of the number n is between 700 and 800.

5. Process according to any of claims 1 to 4, wherein n is the product of at least two primes (p and q) and wherein the modulo n calculations are performed according to the "Chinese remainders" method.

6. Message signature process intended for a signatory (A) provided with a public key v and a secret key s, these keys being related via a modulo n calculation, where n is an integer called modulus,

English translation of the amended sheets of International Preliminary Examination Report

which is specific to the signatory, the said process involving means to calculate an opening c that is notably function of the message M to be signed, able to calculate a number y that is a function of the secret key, and able to transmit the numbers y and c that are the signature of the message M and the message M, the process being characterised in that the modulo n operation is $v=s^{-t} \pmod n$, t being a parameter.

7. Signature process according to claim 6, wherein the signatory selects an integer r at random, which is between 1 and n-1, calculates a parameter x equal to $r^t \pmod n$, calculates a number c that is a function of parameter x and message M to be signed, calculates a number y using its secret key s, the said number y being a function of numbers r and e, and transmits the numbers c and y as signature.

Abstract

Authentication and signature process with reduced number of calculations.

The process involves a first entity called the "prover", which possesses a public key v and a secret key s, these keys verify the relation $v = s^{-t} \pmod{n}$, where n is an integer called modulus and t is a parameter, and a second entity called a "verifier", which knows the public key v. This process implies exchange of information following a "zero-knowledge protocol" between the verifier and the prover and cryptographic calculations on this information, some calculations being carried out "modulo n". The process of the invention is characterised by the fact that the modulus n is specific to the prover that communicates this modulus to the verifier.

SP 16207 C/RS

Declaration, Power Of Attorney and Petition

WE (I) the undersigned inventor(s), hereby declare(s) that :

My residence, post office address and citizenship are as stated below next to my name,

We (I) believe that we are (I am) the original, first, and joint (sole) inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Authentication or signature process with a reduced calculations set

the specification of which

- ☐ is attached hereto.
- ☐ was filed on
  as Application Serial No.
  and amended on
- ☒ was filed as PCT international application
  Number PCT/FR00/00174
  on January 26, 2000
  and was amended under PCT Article 19
  on September 28, 2000

We (I) hereby state that we (I) have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We (I) acknowledge the duty to disclose information known to be material to the patentability of this application as defined in Section 1.56 of Title 37 Code of Federal Regulations.

We (I) hereby claim foreign priority benefits under 35 U.S.C. § 119 (a)-(d) or § 365 (b) of any foreign application(s) for patent or inventor's certificate, or § 365 (a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed. Prior Foreign Application (s)

Application No.	Country	Day/month/Year	Priority Claimed
99 00887	FRANCE	27 January 1999	☒ YES ☐ NO
			☐ YES ☐ NO
			☐ YES ☐ NO
			☐ YES ☐ NO

We (I) hereby claim the benefit under Title 35, United States Code, § 119 (e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

We (I) hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of prior application and the national or PCT International filing date of this application.

Application Serial No.	Filing Date	Status (pending, patented, abandoned)

And we (I) hereby appoint : Norman F. Oblon, Registration Number 24,618; Marvin J. Spivak, Registration Number 24,913; C, Irvin McClelland, Registration Number 21,124; Gregory J. Maier, Registration Number 25,599; Arthur I. Neustadt, Registration Number 24,854; Richard D. Kelly, Registration Number 27,757; James D. Hamilton, Registration Number 28,421; Eckhard H. Kuesters, Registration Number 28,870; Robert T. Pous, Registration Number 29,099; Charles L. Gholz, Registration Number 26,395; William E. Beaumont, Registration Number 30,996; Jean-Paul Lavalleye, Registration Number 31,451; Stephen G. Baxter, Registration Number 32,884; Richard L. Treanor, Registration Number 36,379; Steven P. Weihrouch, Registration Number 32,829; John T. Goolkasian, Registration Number 26,142; Richard L. Chinn, Registration Number 34,305; Steven E. Lipman, Registration Number 30,011; Carl E. Schlier, Registration Number 34,426; James J. Kulbaski, Registration Number 34,648; Richard A. Neifeld, Registration Number 35,299; J. Derek Mason, Registration Number 35,270; Surinder Sachar, Registration Number 34,423; Christina M. Gadiano, Registration Number 37,628; Jeffrey B. McIntyre, Registration Number 36,867; William T. Enos, Registration Number 33,128; Michael E. McKabe Jr., Registration Number 37,182, Bradley D. Lytle, Registration Number 40,073 and Michael R. Casey Registration Number 40,294 ; our (my) attorneys, with full powers of substitution and revocation, to prosecute this application and to transact all business in the Patent Office connected therewith; and we (I) hereby request that all correspondence regarding this application be sent to the firm of OBLON, SPIVAK, McCLELLAND, MAIER & NEUSTADT, P.C., whose post Office Address is : Fourth Floor, 1755 Jefferson Davis Highway, Arlington, Virginia 22202. Customer No. 22850

We (I) declare that all statements made herein of our (my) own knowledge are true and that all statements made on information and belief are believed to be true ; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardise the validity of the application or any patent issuing thereon.

1 - 00 GIRAULT Marc

NAME OF FIRST SOLE INVENTOR

Signature of Inventor

July 09, 2001

Date

Residence : 4 rue Viviane

14000 CAEN (FRANCE) FR

Citizen of : FRANCE

Post Office Address : The same as residence

(2)
over

PAILLES Jean-Claude

NAME OF SECOND INVENTOR

[signature]

Signature of Inventor

July 09, 2001

Date

Residence : 4 Rue des Loisirs

14610 EPRON FRX

FRANCE

Citizen of : France

Post Office Address : The same as residence

NAME OF THIRD INVENTOR

Signature of Inventor

Date

Residence :

Citizen of :

Post Office Address : The same as residence

NAME OF FOURTH INVENTOR

Signature of Inventor

Date

Residence :

Citizen of :

Post Office Address : The same as residence

NAME OF FIFTH INVENTOR

Signature of Inventor

Date

Residence :

Citizen of :

Post Office Address : The same as residence